



# Department of Homeland Security Daily Open Source Infrastructure Report for 24 February 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- Reuters reports the federal Energy Information Administration warns that the East Coast and Texas regions that use reformulated gasoline may face local supply disruptions and price spikes as oil refineries switch to blending the motor fuel with ethanol. (See item [2](#))
- CNN reports a former Internet company officer has been sentenced to eight years in prison on 120 counts of unauthorized access of a protected computer, two counts of access device fraud, and one count of obstruction of justice, in a massive theft of personal data from Acxiom Corporation, which manages personal, financial, and corporate data. (See item [9](#))

## DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *February 22, Federal Energy Regulatory Commission* — **FERC extends lifting of natural gas rules to further hurricane recovery efforts.** On Wednesday, February 22, the Federal Energy Regulatory Commission (FERC) extended the deadline by four months — to February 28, 2007 — for the completion of construction of certain infrastructure projects pursuant to the Commission's waiver of regulations raising blanket certificate limits. The Commission's waiver is intended to help mitigate natural gas supply disruptions caused by Hurricanes Katrina and Rita. The Commission said lifting certain restrictions for an extended period is intended to

afford additional time for facilities that cannot be placed in service by the beginning of the 2006–2007 heating season to be completed in time to deliver more gas services during the heating season when the facilities are most needed. "Recovery of infrastructure in the Gulf of Mexico is proceeding apace. This action should further encourage those efforts," said Chairman Joseph T. Kelliher. The Commission cited information from the U.S. Minerals Management Service that indicates that 400 million cubic feet of natural gas production is expected to remain offline by the start of the 2006–2007 hurricane season.

Source: <http://www.ferc.gov/press-room/press-releases/2006/2006-1/02-22-06.asp>

2. *February 22, Reuters* — **EIA says fuel supply problems seen.** The U.S. East Coast and Texas regions that use reformulated gasoline may face local supply disruptions and price spikes as oil refineries switch to blending the motor fuel with ethanol, the federal Energy Information Administration (EIA) warned on Wednesday, February 22. The government in May will no longer require refineries to use in gasoline oxygenates like MTBE (methyl tertiary butyl ether), banned in many states for polluting drinking water. Many refineries plan to stop using MTBE before the summer season begins and switch to clean-burning ethanol that is made mostly from corn. However, EIA said U.S. ethanol production is running near capacity and "is not adequate to replace the MTBE lost." As a result, the EIA said the East Coast, particularly Maryland, Delaware, and Virginia, and the Texas cities of Houston and Dallas, may face tight gasoline supplies and higher fuel prices for reformulated gasoline (RFG). The agency said, "Overall, the complexity of the transition away from MTBE-blended RFG may give rise to local imbalances between supply and demand and associated price surges during the change... the tight supply situation is not likely to ease significantly, leaving the market exposed to the increased potential for price volatility..."

Report: [http://www.eia.doe.gov/pub/oil\\_gas/petroleum/feature\\_article/s/2006/mtbe2006/mtbe2006.pdf](http://www.eia.doe.gov/pub/oil_gas/petroleum/feature_article/s/2006/mtbe2006/mtbe2006.pdf)

Source: [http://news.yahoo.com/s/nm/20060222/bs\\_nm/energy\\_mtbe\\_ethanol\\_dc\\_4](http://news.yahoo.com/s/nm/20060222/bs_nm/energy_mtbe_ethanol_dc_4)

3. *February 22, Agence France–Press* — **IEA official says unrest overshadows Iraqi oil production.** An International Energy Agency (IEA) official said recently at a conference in Prague entitled "Energy Security – The NATO Forum on Energy Security Technology" that the IEA does not believe Iraq can boost oil production to predicted levels because of unrest in the country. "We do not think that it is possible in the absence of security and order for major oil companies to come to invest in Iraq," IEA's chief economist, Fatih Birol, said on Wednesday, February 22. Birol also said that "we will face tighter energy markets and higher prices for years to come," adding that the world faced a "troubled energy picture." Iraqi oil production, currently at 1.6–1.7 million barrels a day, could rise to three million barrels a day by 2010, but this would fall short of a forecast by Iraq of six million barrels a day, he said. Birol added that the agency doubted whether foreign investment would allow Iran to double its current production of about four million barrels a day by 2030, because of tension surrounding its plans to develop nuclear power. Saudi Arabia had enough reserves and production capacity to meet increased world demand by boosting current production of about 11 million barrels a day to 18 million barrels a day by 2030 but it might choose not to do so, Birol said.

Source: [http://news.yahoo.com/s/afp/20060222/wl\\_mideast\\_afp/iraqenergyoiloutput\\_060222143029](http://news.yahoo.com/s/afp/20060222/wl_mideast_afp/iraqenergyoiloutput_060222143029)

4.

*February 21, PostStar (NY)* — **Public Service Commission assessing National Grid response to outage.** The New York state Public Service Commission has begun a review of National Grid's response to the Friday, February 18, windstorm that left more than 213,000 customers in its New York service territory without power, commission spokesperson David Flanagan said. Such a review is automatic any time power is out for three days or longer. About 4,800 National Grid customers were still without service as of 4:30 p.m. EST Tuesday, February 21, mostly in Saratoga, Warren, and Washington counties, the company reported. National Grid has 60 days to submit its own evaluation of its response to the commission, Flanagan said, but the Public Service Commission has already begun a review, which will continue until National Grid submits its report. "We would make recommendations to address any improvements that we see," he said. State Assemblyperson Teresa Sayward, who filed a complaint about National Grid, urged Public Service Commission Chairman William Flynn to require National Grid to purchase generators for all schools in the company's service territory, so school buildings could be used as emergency shelters in the event of future outages. Source: <http://www.poststar.com/story.asp?storyid=211621>

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

Nothing to report.

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

### **5. *February 23, Aviation Week* — JTRS Program expecting acquisition memo from Pentagon.**

The Joint Tactical Radio System (JTRS) program expects soon to receive an acquisition decision memorandum signed by Pentagon acquisition chief Ken Krieg that will formally approve the program's restructuring, according to JTRS Ground Radio Program Manager Col. Andrew Dwyer. "That should be signed any day or week now," Dwyer said during the Institute for Defense and Government Advancement's Software Radio conference Wednesday, February 22. JTRS is developing a family of interoperable software-defined military radios. The Pentagon considered canceling Boeing's prime contract for JTRS Cluster 1 last year, in response to the program's cost and schedule problems. The JTRS Joint Program Executive Office presented three spiral development options for Krieg to choose from. The new plan provides a "networking plus legacy waveform software-defined radio capability" with six waveforms in JTRS increment one, while slipping some capabilities to increment two, Dwyer said. The new plan is an evolutionary rather than "big bang" approach, he said. The re-baselined JTRS program will follow the new "golden rule" established for the program by Krieg, which is "do not promise something that you can't deliver," Dwyer said. "It should be a moderate-risk schedule. Don't sign up again for a high-risk schedule."

Source: [http://www.aviationnow.com/avnow/news/channel\\_netdefense\\_story.jsp?id=news/JTRS02236.xml](http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?id=news/JTRS02236.xml)

### **6. *February 22, U.S. Army* — New center to drive Army modernization.** Secretary of the Army Dr. Francis J. Harvey recently directed the formation of the Army Capabilities Integration

Center, known as ARCIC, from the resources and organization of the U.S. Army Training and Doctrine Command Futures Center. The ARCIC will be the lead Army agency to coordinate and integrate war-fighting capabilities among all the military services and other agencies and be located at Fort Monroe, VA. The newly designed ARCIC will develop and integrate the Army's capability requirements. Today, the Army is moving from the current force to the future force through a modernization program called the Future Combat Systems (FCS). FCS provides soldiers with leading-edge technologies to improve their capabilities to fight the enemy in complex environments. ARCIC will ensure that FCS capabilities are fielded as soon as practical across the force.

Source: [http://www4.army.mil/ocpa/read.php?story\\_id\\_key=8613](http://www4.army.mil/ocpa/read.php?story_id_key=8613)

[\[Return to top\]](#)

## **Banking and Finance Sector**

7. *February 23, Computer Crime Research Center* — **UK report finds indirect costs of online fraud are still high.** A report released by CyberSource addressed the prevalence, detection, prevention and management of online fraud in relation to UK businesses. In total, one hundred and sixty merchants took part in the survey, which was conducted over two weeks in September 2005. The results indicate that the struggle against online fraud has now been almost universally recognized as an issue central to the future success of web-borne commerce. Companies are continuing to take appropriate steps and would appear to be treating the threat ever more seriously. The report found that credit cards are still the number one payment preference; fraud has moved further up merchants' online agendas; revenue growth is outstripping fraud increases; merchants are mindful of evolving scammer methodologies; and the indirect costs of online fraud are still high. The UK survey also found that one percent of accepted orders turned out to be fraudulent, down from 1.6 percent in the 2004 survey. This matches the U.S. finding of one percent, a decrease of 0.3 percent from last year's result, suggesting that organizations on both sides of the Atlantic are starting to manage their risk processes more effectively.

UK Fraud Report: <http://www.thepowerofpayment.co.uk/fraudreport20062/download/s/fraudreport2006.pdf>

Source: <http://www.crime-research.org/news/23.02.2006/1841/>

8. *February 22, Websense* — **Phishing attack targets First American Bank.** Websense Security Labs has received reports of a new phishing attack that targets customers of First American Bank. Users receive a spoofed e-mail, which claims that their account will be deactivated unless certain actions are taken. The message provides a link to a phishing Website where users are prompted to enter personal account information. The phishing site is hosted in the United States and was up at the time of this alert. The e-mail reads in part: "This is your official notification from First American Bank that the service(s) listed below will be deactivated and deleted if not renewed immediately. Previous notifications have been sent to the Billing Contact assigned to this account. As the Primary Contact, you must renew the service(s) listed below or it will be deactivated and deleted."

Source: <http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=429>

9.

*February 22, CNN* — **Florida man sentenced to eight years in data theft; stole over a billion records.** A former officer of an Internet company was sentenced Wednesday to eight years in prison in a massive theft of personal data from Acxiom Corporation, which manages personal, financial and corporate data, federal prosecutors announced Wednesday, February 22. Scott Levine was sentenced on 120 counts of unauthorized access of a protected computer, two counts of access device fraud and one count of obstruction of justice, according to the U.S. Justice Department. Levine, of Boca Raton, Fla., was the controlling owner of Snipermail, Inc., a corporation which engaged in distributing advertisements over the Internet to e-mail addresses. From January through July 2003, prosecutors said, he stole more than a billion records containing personal information such as names, mailing and e-mail addresses and phone numbers of Acxiom Corporation clients. "Levine used sophisticated decryption software to illegally obtain passwords and exceed his authorized access to Acxiom databases, which contained information belonging to Acxiom's clients," a statement from the Justice Department said. There is no evidence that the data sold by Levine or others associated with the investigation was used in identity theft or credit card schemes, authorities said, but some of it was resold to a broker for use in an ad campaign.

Source: [http://money.cnn.com/2006/02/22/news/data\\_theft/index.htm?section=money\\_latest](http://money.cnn.com/2006/02/22/news/data_theft/index.htm?section=money_latest)

10. *February 22, Sentinel (PA)* — **Chemicals force Pennsylvania bank evacuation.** A Carlisle, PA bank was evacuated Tuesday morning, February 21, after an employee found chemicals in the night depository box that were feared to be explosive if mixed, Carlisle Mayor Kirk Wilson says. The seven or eight employees at Wachovia at 604 E. High St. were evacuated after one reported feeling ill from the vapors, Wilson says. Carlisle Fire Chief Robert Kennedy cleared the bank at 10:20 a.m. EST, sealing off the depository box and the remaining chemicals inside. Most of the chemicals were seized by a forensic specialist. The chemicals were apparently dropped off some time over the long President's Day weekend, Wilson says. Police are "looking into a number of possibilities to identify the culprit," he says.

Source: <http://www.cumberlink.com/articles/2006/02/22/news/news27.txt>

11. *February 22, Daily Journal (NJ)* — **Scam targets New Jersey bank customers.** Sun National Bank began mailing warnings to its 90,000 customers Tuesday, February 22, alerting them to a scam in which e-mails purportedly sent by the bank asked customers to submit personal information through a fake Website. The phony e-mails began appearing in the inboxes of customers and non-customers on Friday, February 18. It said the message was sent by Sun National Bank and carried a warning saying that the recipients' banking services would be deactivated and deleted from the system if personal information was not immediately confirmed online. Recipients who clicked on the links provided in the scam e-mail were taken to a fake Web page designed to look almost exactly like Sun's online banking login page. If the person logged into the page, he was then asked to submit ATM card numbers and associated pin numbers. Ed Malandro, Sun's senior vice president and director of marketing, said, "At no time was our Internet banking service ever compromised...only four customers responded to this e-mail and only one was financially impacted, but it was minimal." Malandro said "Someone in Seattle, WA, forwarded the e-mail to us indicating they thought it was a scam," Malandro said.

Source: <http://www.thedailyjournal.com/apps/pbcs.dll/article?AID=/20060222/NEWS01/602220310/1002>



12. *February 22, Agence France–Press* — **Twelve Nigerians arrested in Holland for Internet scam.** Dutch police said they had arrested 12 Nigerians in connection with an Internet scam in which e-mails were sent to Americans tricking them into investing in non-existent schemes. The Nigerians were detained on suspicion of committing fraud or involvement in fraud in the scheme, which earned them a total of two million dollars. They were arrested Tuesday, February 21 after raids in Amsterdam, Holland and the city of Zaandam, during which police seized thousands of dollars in cash, computers, and fake travel documents. Most of the victims of the scam were U.S. citizens. Four of the men detained were arrested on the request of U.S. authorities. The gang posted some 100,000 e-mails to potential victims, police said.  
Source: [http://news.yahoo.com/s/afp/20060222/tc\\_afp/netherlandsnigeriaus:\\_ylt=ApLxFSHCDDzey5fDpwUt3UQjtBAF:\\_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhda](http://news.yahoo.com/s/afp/20060222/tc_afp/netherlandsnigeriaus:_ylt=ApLxFSHCDDzey5fDpwUt3UQjtBAF:_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhda)

[[Return to top](#)]

## **Transportation and Border Security Sector**

13. *February 23, Government Accountability Office* — **GAO–06–295: Border Surveillance Technology Program (Report).** In September 2004, the Department of Homeland Security (DHS) established America's Shield Initiative (ASI) — a program that included a system of sensors, cameras, and databases formerly known as the Integrated Surveillance Intelligence System (ISIS) — to detect, characterize, and deter illegal breaches to the northern and southern U.S. borders. The goals of the ASI program were to address ISIS capability limitations and support the department's antiterrorism mission. In April 2005, department officials told the Government Accountability Office (GAO) that ISIS was subsumed within ASI. By congressional mandate, GAO reviewed the program to determine (1) the operational needs that ASI was intended to address and DHS's plans for ASI, (2) the steps that DHS had taken to ensure that ASI was aligned with the department's enterprise architecture, and (3) the actions that DHS had taken to establish the capability to effectively manage ASI. In written comments, DHS agreed with a draft of this report, stating that it was factually correct in virtually all aspects. DHS also commented that it has ceased work on ASI and redirected resources to its Secure Border Initiative. It also described program management corrective actions that it plans to implement

Highlights: <http://www.gao.gov/highlights/d06295high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-295>

14. *February 23, Chicago Tribune* — **US Airways looking to profit.** Only two of the nation's large, mainline airlines are projecting that 2006 will be a profitable year. It is no coincidence that the two, United Airlines and US Airways, also are carriers that recently left bankruptcy protection. US Airways reported a loss of \$537 million for 2005 on Tuesday, February 21, but said it, too, anticipates a turnaround this year, said Chairman and Chief Executive Doug Parker. Of the six legacy carriers — mainline airlines that offer domestic and international routes — Northwest Airlines and Delta Air Lines are operating in bankruptcy. Two others, American Airlines and Continental Airlines, have said that turning a profit remains a challenge. High fuel prices and intense competition from discount carriers have hammered the airline industry. Even low-cost carriers have found it difficult to make a profit. Southwest Airlines, the nation's most successful carrier by most measures, made money last year only because it has an extensive

system for locking in prices for much of its fuel needs years in advance. The airlines that have gone through bankruptcy shed billions of dollars in wage and benefit costs. United and US Airways also dumped their pension plans, replacing them with less expensive retirement plans. Source: <http://www.chicagotribune.com/business/chi-0602220057feb22.1.4331940.story?ctrack=1&cset=true>

15. *February 23, Houston Business Journal* — **Continental to return to full service in New Orleans.** Continental Airlines plans to return to its pre-Hurricane Katrina frequency of 111 flights per week at Louis Armstrong New Orleans International Airport by May. The new flights to be added in May will lift Continental to 94 percent of pre-Katrina capacity. Source: <http://biz.yahoo.com/bizj/060222/1231538.html?.v=1>

16. *February 22, Department of Homeland Security* — **Fact Sheet: Securing U.S. ports.** Following 9/11, the federal government has implemented a multi-layered defense strategy to keep U.S. ports safe and secure. New technologies have been deployed with additional technologies being developed and \$630 million has been provided in grants to the largest ports, including \$16.2 million to Baltimore; \$32.7 million to Miami; \$27.4 million to New Orleans, \$43.7 million to New York/New Jersey; and \$15.8 million to Philadelphia. This Fact Sheet provides information such as Who Secures The Ports; the Layered Defense for ports; Recommended Standards for Container Security Initiative; and other port security matters. Source: <http://www.dhs.gov/dhspublic/display?content=5437>

[[Return to top](#)]

## **Postal and Shipping Sector**

17. *February 23, DMNews* — **USPS headed for \$1.8 billion loss this year.** The U.S. Postal Service (USPS) expects to lose \$1.8 billion by the end of its fourth quarter, in part because of surprisingly weak Standard mail volume. "We see very little growth in Standard mail volume [right now], [but] we are hoping to get it back up to the three percent growth level that it did last year," Richard J. Strasser Jr., USPS chief financial officer and executive vice president, said at the quarterly Mailers' Technical Advisory Committee meeting held on Wednesday, February 22. Strasser gave his final MTAC presentation before retiring April 3. From October 1, 2005, to January 31, 2006, the USPS planned for a Standard mail increase of 4.7 percent; the actual increase, however, was 1.5 percent. First-Class mail was the only category to drop in volume: down 1.6 percent. Fuel costs, up 20 percent to 30 percent, are becoming a big concern for postal officials. The costs affect the agency's cost-of-living expenses. Source: [http://www.dmnews.com/cgi-bin/artprevbot.cgi?article\\_id=35818](http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=35818)

[[Return to top](#)]

## **Agriculture Sector**

18. *February 23, Associated Press* — **Agriculture experts talk about border threats.** Border states and neighboring countries must cooperate because threats to the food supply don't recognize boundaries, according to experts who are attending a conference in La Cruces, NM.

The first Border Governor's Agriculture Tabletop conference, dedicated to outlining shared dangers to agriculture along the border, has attracted about 140 experts from 11 U.S. and Mexican border states. Several attendees said the most important result that will come from the conference is understanding how different states plan to respond to a threat. "Because we're here, we can go one-on-one and get a feel for what's going on in New Mexico and Texas ...," said Don Butler, director of the Arizona Department of Agriculture. "This is the first time we've gone across the lines and done this, which is great." On Tuesday, February 21, attendees completed a training session on an emergency-response protocol being promoted by the federal government.

Source: <http://www.dfw.com/mld/startelegram/news/state/13940625.htm>

19. *February 23, Agricultural Research Service* — **Watermelon line may help breeders combat mildew.** Agricultural Research Service (ARS) researchers and cooperators are introducing watermelon stock that may help breeders combat powdery mildew, a disease that threatens watermelon yields and quality in several states. Recently, two races of powdery mildew have been reported on watermelon, and they appear to be geographically separate. Existing watermelon lines, which were thought resistant, were found to be susceptible. But ARS researchers discovered the first documented resistance to race 1 powdery mildew in an ARS germplasm collection. According to Angela Davis, geneticist at the ARS South Central Agricultural Research Laboratory in Lane, OK, watermelon has historically been resistant to powdery mildew, but the disease has become widespread during the past few years. A significant problem in Europe and Africa for about a decade, powdery mildew has emerged as a severe problem in some areas of the U.S. Powdery mildew appears as a dusty white or gray coating over leaf surfaces or other plant parts, and can be difficult to control. The new watermelon line may be useful for introducing resistance to race 1 powdery mildew (caused by the fungus *Podosphaera xanthii*) into commercial watermelon cultivars.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

20. *February 22, Stop Soybean Rust News* — **Six kudzu patches green in Montgomery, four have rust.** Kudzu is alive and green in inner-city Montgomery, AL, and four of six patches observed Wednesday, February 22, were infected with soybean rust. Montgomery County was the site of the first discovery of Asian soybean rust in the U.S. this year on January 12. Rust was found in two more Alabama counties, Baldwin and Mobile, on February 15. Ed Sikora, Auburn University professor and Extension plant pathologist, said that three small kudzu patches with green tissue were observed in the city of Montgomery, as scouts checked on how kudzu fared through recent cold weather. Each of the new patches found was located near the south-southeast side of a building. Two of the three patches also had old growth that was infected with soybean rust, Sikora said. The third patch had new (2006) growth, but did not show symptoms of the disease. Three other kudzu patches that had first been observed in the city in mid-January were also scouted, and each still retained green tissue. Two of these patches were infected with rust and showed signs of new growth.

Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=691>

21. *February 22, Associated Press* — **Soybean rust found on soybeans in Hidalgo County, TX.** Asian soybean rust has been found on soybeans in the western-most U.S. location yet — Weslaco, TX, in Hidalgo County, just a few miles north of the Mexican border. The field was harvested February 14, so it won't serve as a source of inoculum, officials said. Texas A&M



Extension plant pathologist Tom Isakeit reported the rust was found on soybeans growing in a one-acre field at the Texas A&M Experiment Station in Weslaco. He had surveyed the field in December 2005, but did not see any symptoms of rust then. On February 14, the find was reported by plant pathologist Marvin Miller after he examined a sample brought in by his technician, Robert Saldana. On February 16, the finding was confirmed with testing by the Texas Plant Disease Diagnostic Clinic. There are now 17 U.S. counties where soybean rust has been confirmed in 2006. Hidalgo County is the first in Texas this year. Last year, the only confirmed soybean rust in Texas 330 miles to the northeast — on kudzu in the southeast Texas county of Liberty, north of Galveston.

Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=690>

[\[Return to top\]](#)

## **Food Sector**

**22. *February 22, U.S. Food and Drug Administration* — Infant formula recall.** The U.S. Food and Drug Administration (FDA) is alerting the public to a recall being conducted by Mead Johnson for their GENTLEASE powdered infant formula, lot number: BMJ19. This lot was found to contain metal particles, consisting of up to 2.7 millimeter in size. No illnesses have been reported to date. However, in the rare instance that an infant were to inhale the infant formula into the lungs, the presence of these particles could present a serious risk to the infant's respiratory system and throat. There were approximately 41,464 24-ounce cans of this lot of recalled product distributed, beginning on December 16, 2005, through many major retail stores across the country, so the consumer should concentrate on the code on the can rather than on the place of purchase. Mead Johnson informed the FDA of this problem. FDA and Mead Johnson are currently investigating the cause of the metal particles found in the infant formula in this highly unusual incident.

Source: <http://www.fda.gov/bbs/topics/NEWS/2006/NEW01323.html>

[\[Return to top\]](#)

## **Water Sector**

**23. *February 23, Bloomberg* — China's water shortage may spur rural unrest, threaten growth.** China's burgeoning cities are siphoning water away from farmers, undermining government pledges to improve living standards in the countryside — home to 70 percent of the nation's 1.3 billion people. Rural water shortages threaten to stoke unrest, cut harvests, and slow the expansion of the world's fastest-growing major economy. The government is building a \$62 billion project to move water to arid northern provinces from the south and central regions. "China's water shortage reflects the nation's growing urban-rural wealth gap," says Andy Xie, chief China economist at Morgan Stanley in Hong Kong. "China has to ensure its rural majority has access to water supplies or it may face unrest." China is a dry country to begin with, averaging about 2,200 cubic meters of water per person, a quarter of the world average, the Ministry of Water Resources says. Economic development has increased competition for scarce supplies. Factories and urban residents used 34 percent of the nation's water in 2004, up from 25 percent in 1998, according to the Ministry of Water Resources. That

has cut grain production, which fell 8.4 percent to 469.4 million tons during the same period, according to the National Bureau of Statistics.

Source: <http://www.bloomberg.com/apps/news?pid=10000080&sid=aWVfESld0zwQ&refer=asia>

[\[Return to top\]](#)

## **Public Health Sector**

**24. February 23, Washington Post — Wider flu vaccination urged.** The committee that sets federal immunization policy recommended Wednesday, February 22, that children two to five years old be vaccinated against influenza every year, expanding the "target population" for flu shots and inching toward the day when they will be recommended for everyone. The government had previously recommended yearly flu vaccination only for children age six months to 23 months. The new recommendation also includes "household contacts" of children between their second and fifth birthdays. This group — parents and older siblings not covered by other recommendations — outnumbers the children in the new recommendation. Flu vaccination has been urged for years for everyone older than 50, with special attention to people over 65 and those with chronic illnesses. Children older than six months with chronic illnesses should also be immunized. The decision may have secondary benefits, as well. Recent studies show that vaccinating children may help protect the elderly and chronically ill, who are at highest risk from flu complications. Children are principally responsible for spreading the germ, and with less of it circulating, fewer people will become infected.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/22/AR2006022202080.html>

**25. February 23, Agence France–Presse — Deadly bird flu strain found in Slovakia for first time.** The deadly H5N1 strain of bird flu has been detected for the first time in Slovakia in two wild birds. "Bird flu has been confirmed in Slovakia," Agriculture Minister Zsolt Simon said at a news conference. Slovakia becomes the eighth European Union country to declare the presence of the H5N1 virus following Hungary, Slovenia, Austria, Greece, Italy, France, and Germany. The presence of the virus was confirmed by the Slovak Veterinary Office in a duck and a falcon found dead Monday, February 20, at Bratislava and the town of Gabčíkovo the minister said Thursday, February 23. Samples have been sent to the European Union's central laboratories in Britain for confirmation with the results expected in the next days, he added.

Source: [http://news.yahoo.com/s/afp/20060223/hl\\_afp/healthfluslovakia\\_060223131829;\\_ylt=Aql\\_jz3s2ZmBJJzw20u4baJOrgF;\\_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--](http://news.yahoo.com/s/afp/20060223/hl_afp/healthfluslovakia_060223131829;_ylt=Aql_jz3s2ZmBJJzw20u4baJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--)

**26. February 23, Reuters — Superbug deaths up 22 percent in England and Wales.** The number of deaths linked to the deadly superbug methicillin-resistant *Staphylococcus aureus* (MRSA) rose by nearly a quarter between 2003 and 2004 in England and Wales, figures showed on Thursday, February 23, adding to fears over the spread of the infection. Mentions of MRSA on death certificates jumped 22 percent to 1,168 in 2004 from 955 the year before, the Office of National Statistics (ONS) said. MRSA, a bacteria resistant to certain antibiotics, was given as the underlying cause of death in 360 cases, up from 195 cases in 2000. On Monday, February 20, the British Medical Association advised doctors to stop wearing ties and traditional white

coats because they might be responsible for spreading hospital superbugs. MRSA was first detected in 1961, the same year as the antibiotic methicillin was first used. The ONS said MRSA contributed to two out of every 1,000 deaths in England and Wales, and to 3 of every 1,000 deaths in NHS hospitals and nursing homes.

MRSA information: [http://www.cdc.gov/ncidod/diseases/submenus/sub\\_mrsa.htm](http://www.cdc.gov/ncidod/diseases/submenus/sub_mrsa.htm)

Source: [http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006-02-23T144458Z\\_01\\_L23243030\\_RTRUKOC\\_0\\_US-BRITAIN-MRSA.xml](http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006-02-23T144458Z_01_L23243030_RTRUKOC_0_US-BRITAIN-MRSA.xml)

27. *February 23, BBC* — **Animal link in anthrax case.** A New York-based dancer has contracted respiratory anthrax, apparently after inhaling spores from raw animal hides used on drums. Vado Diamande is in hospital in a stable condition after collapsing during a performance in Pennsylvania. Diomande recently traveled to Africa to collect skins. Diomande's apartment has been searched for samples of the hides. He is thought to have inhaled anthrax spores while treating the hides, though it is not clear whether infection occurred in Africa or the U.S. Investigators have been testing hides for contamination at his apartment in New York City. Source: <http://news.bbc.co.uk/2/hi/americas/4743606.stm>

[[Return to top](#)]

## **Government Sector**

28. *February 23, The White House* — **The Federal Response to Hurricane Katrina: Lessons Learned.** The Administration has released its review of the federal response to Hurricane Katrina. The President's charge to evaluate the federal government's response to the storm resulted in the report and recommendations released on Thursday, February 23, entitled, The Federal Response to Hurricane Katrina: Lessons Learned. The product of an extensive review, led by the President's Homeland Security Advisor Fran Townsend, the Report identifies deficiencies in the federal government's response and lays the groundwork for transforming how the nation — from every level of government, to the private sector, to individual citizens and communities — pursues a real and lasting vision of emergency preparedness and response. The Report assesses the federal response, identifies lessons learned, and recommends appropriate corrective actions. The Report identifies the systemic problems in Federal emergency preparedness and response revealed by Hurricane Katrina — and the best solutions to address them. Where actions at the state and local level had bearing on federal decisions or operations, they are included in order to provide full context. Lessons Learned Fact Sheet: <http://www.whitehouse.gov/news/releases/2006/02/20060223.html>  
Source: <http://www.whitehouse.gov/reports/katrina-lessons-learned/>

29. *February 23, Department of Homeland Security* — **Statement by Secretary Chertoff regarding Katrina Lessons Learned Report.** Concerning the report released by The White House on Thursday, February 23, Department of Homeland Security Secretary Michael Chertoff said, "I commend Fran Townsend for leading a thorough and comprehensive after action review of the government's response to Hurricane Katrina. The Department of Homeland Security (DHS) participated actively in this effort. We have already begun to take action to address many of the issues raised in the report, particularly those areas we need to

improve before the start of the 2006 hurricane season. This report is consistent with the Second Stage Review plan we announced in July as well as the Federal Emergency Management Agency improvements we recently announced. It will help our shared efforts to build a more integrated DHS and a more seamless federal disaster management system. I look forward to working with Fran and the Homeland Security Council to assess and address these important recommendations.”

Source: <http://www.dhs.gov/dhspublic/display?content=5438>

[\[Return to top\]](#)

## **Emergency Services Sector**

30. *February 23, Government Accountability Office* — **GAO-06-467T: Emergency Preparedness and Response: Some Issues and Challenges Associated with Major Emergency Incidents (Testimony).** In a testimony before California's Little Hoover Commission, William O. Jenkins, Jr., Director of Homeland Security and Justice Issues, discusses the challenges of effective emergency preparedness for, response to, and recovery from major emergencies, including catastrophic events. According to Jenkins, the biggest challenge in emergency preparedness is getting effective cooperation in planning, exercises, and capability assessment and building across first responder disciplines and intergovernmental lines. With regard to the status of emergency preparedness across the nation, we know relatively little about how states and localities (1) finance their efforts in this area, (2) have used their federal funds, and (3) are assessing the effectiveness with which they spend those funds. As the nation assesses the lessons of Katrina, we must incorporate those lessons in assessing state and local emergency management plans, amend those plans as appropriate, and reflect those changes in planned expenditures and exercises. This effort requires clear priorities, hard choices, and objective assessments of current plans and capabilities. Failure to address these difficult tasks directly and effectively will result in preparedness and response efforts that are less effective than they should and can be.

Source: <http://www.gao.gov/new.items/d06467t.pdf>

[\[Return to top\]](#)

## **Information Technology and Telecommunications Sector**

31. *February 23, Associated Press* — **China claims 400 million mobile phone users.** China's mobile phone market, already the world's biggest, has passed 400 million users, the government said Thursday, February 23. The number of subscribers on the country's mainland rose 5.4 million in January to 398 million, the official Xinhua News Agency reported, citing the Ministry of Information Industry. It said that with further growth this month, the total number has hit 400 million by this point, though it didn't give an exact figure.

Source: [http://news.yahoo.com/s/ap/20060223/ap\\_on\\_hi\\_te/china\\_mobile\\_phones:\\_ylt=AqM8uSiHtGFGjd.QOyx8.BIjtBAF:\\_ylu=X3oDMTA5aHJvM\\_DdwBHNIYwN5bmNhdA--](http://news.yahoo.com/s/ap/20060223/ap_on_hi_te/china_mobile_phones:_ylt=AqM8uSiHtGFGjd.QOyx8.BIjtBAF:_ylu=X3oDMTA5aHJvM_DdwBHNIYwN5bmNhdA--)

*February 22, Security Tracker* — **Mozilla Thunderbird validation error in IFRAME SRC tag lets remote users execute arbitrary javascript.** A vulnerability was reported in Mozilla Thunderbird. A remote user can cause arbitrary scripting code to be executed on the target user's system. Analysis: The software does not properly filter javascript from HTML tags. A remote user can send HTML based e-mail with arbitrary javascript in the SRC attribute of the IFRAME tag. When the target user edits the message (when replying to the message, for example), the javascript will be executed, regardless of the javascript settings in the preferences. Affected versions: 1.0.7 and prior versions.

Solution: The vendor has issued a fixed version (1.5), available at:

<http://www.mozilla.com/thunderbird/>

Source: <http://securitytracker.com/alerts/2006/Feb/1015665.html>

33. *February 22, Associated Press* — **China to crack down on spam.** China is cracking down on junk e-mail and "illegal" mobile phone text messages, the official Xinhua News Agency said Tuesday, February 21. A new regulation will ban sending e-mail for advertising purposes to people without their permission, and all advertising e-mail must be titled "advertisement" or "AD," the agency said. It also said that mobile phones must be registered under users' real names, and that text messaging will be controlled more tightly due to the spread of "illegal messages." They said the measure was aimed at fighting unspecified telephone fraud, and the use of counterfeit and otherwise illegally obtained mobile phones. The government was vague on details, however. For instance, the report did not describe what constituted illegal messages or how they would be controlled, nor did it specify any penalties or say when the new rules would take effect. It's also not clear how well the rules could be enforced. Several countries and U.S. states have anti-spam laws, yet junk e-mail continues to be an online pest, with much of it coming from or through computers in China and other Asian countries.

Source: [http://www.cnn.com/2006/TECH/internet/02/22/china.spam.crack down.ap/index.html](http://www.cnn.com/2006/TECH/internet/02/22/china.spam.crack.down.ap/index.html)

34. *February 22, Network World* — **Study shows how photonic decoys can foil hackers.** A University of Toronto professor and researcher has demonstrated for the first time a new technique for safeguarding data transmitted over fiber-optic networks using quantum cryptography. Professor Hoi-Kwong Lo, a member of the school's Center for Quantum Information and Quantum Control, is the senior author of a study that sheds light on using what's called a photonic decoy technique for encrypting data. Quantum cryptography is starting to be used by the military, banks and other organizations that seek to better protect the data on their networks. This sort of cryptography uses photons to carry encryption keys, which is considered safer than protecting data via traditional methods that powerful computers can crack. Quantum cryptography is based on fundamental laws of physics, such that merely observing a quantum object alters it. Lo's study is slated to appear in the Friday, February 24, issue of Physical Review Letters.

Source: <http://www.networkworld.com/news/2006/022206-quantum-cryptog raphy.html>

35. *February 22, ZDNet UK* — **Security fears over London's blanket Wi-Fi.** Security company McAfee on Tuesday, February 21, raised security concerns over the London's plan to install a Wi-Fi network throughout the Square Mile. The system will be constructed by The Cloud, and should give most of the city's workers wireless access within six months. However, McAfee has raised concerns about the security implications of the project. "Our big concern is that most people care more about connectivity than security. Always-on broadband makes it easier for



hackers to find and target people. There is also a knowledge gap — most people aren't that savvy when it comes to this technology," said Sal Viveros, security expert at McAfee. McAfee recommended that companies prepare themselves for always-on wireless access by learning about the techniques that hackers are using to target susceptible mobile employees, as London is a tempting target for hackers.

Source: <http://news.zdnet.co.uk/internet/security/0.39020375.3925373.0.00.htm>

**36. February 22, IDG News Service — Europe approves powerline communications**

**specification.** Efforts to use electricity cables to transmit data took a step forward in Europe with the publication of an open specification for power line communications. The Open PLC European Research Alliance (OPERA), which is partly funded by the European Commission, said its specification will accelerate the development of products that use power lines for broadband Internet access, voice and video services, as well as utility applications such as automatic meter reading. The approval of the specification, announced Tuesday, February 21, comes after more than two years of development by a consortium of experts from 35 organizations, including 10 universities. Products based on the specification will deliver speeds of more than 200Mbps, according to OPERA. It is based on Orthogonal Frequency Division Multiplexing (OFDM) modulation and offers Frequency Division and Time Division repeating capabilities.

OPERA's report is available for download (click on item D59):

[http://www.ist-opera.org/project\\_outputs\\_available.html.htm](http://www.ist-opera.org/project_outputs_available.html.htm)

Source: <http://www.networkworld.com/news/2006/022206-europe-powerline-specification.html>

### Internet Alert Dashboard

#### DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** US-CERT is aware of publicly available exploit code for a vulnerability in Apple Safari Browser. The Apple Safari browser will automatically open "safe" file types, such as pictures, movies, and archive files. A system may be compromised if a user accesses an HTML document that references a specially crafted archive file. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user.

More information can be found in the following US-CERT Vulnerability Note:

VU#999708 – Apple Safari may automatically execute arbitrary shell commands

Although there is limited information on how to fully defend against this exploit, US-CERT recommends the following mitigation:

Disable the option "Open 'safe' files after downloading," as specified in the Securing Your Web Browser document.

### **Public Exploit Code for Buffer Overflow Vulnerability in Microsoft Windows**

**Media Player Plug-in for Non-IE Browsers** US-CERT is aware of publicly available exploit code for a buffer overflow vulnerability in Windows Media Player plug-in for browsers other than Internet Explorer (IE). For more information can be found in the following US-CERT Vulnerability Note:

VU#692060 – Microsoft Windows Media Player plug-in buffer overflow

<http://www.kb.cert.org/vuls/id/692060>

US-CERT urges users to apply appropriate updates and review the workarounds listed in the Microsoft Security Bulletin MS06-006 to mitigate this vulnerability.

<http://www.microsoft.com/technet/security/Bulletin/MS06-006.mspx>

### **Current Port Attacks**

<b>Top 10 Target Ports</b>	1026 (win-rpc), 6881 (bittorrent), 445 (microsoft-ds), 25 (smtp), 139 (netbios-ssn), 80 (www), 22159 (---), 49200 (---), 135 (epmap), 54000 (---)
----------------------------	---

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

**37. *February 23, Associated Press* — Oregon high school shooting.** A teenager wielding a handgun shot and wounded a 16-year-old student at the high school in Roseburg, OR, on Thursday, February 23, just before classes were to begin. Police chased the shooter down the street to a diner, where he put the gun to his head before surrendering. Police described the shooter as also a 16-year-old, and police spokesperson Sgt. Aaron Dunbar said the shooter appeared to be a student at Roseburg High School. Students, teachers and administrators saw the shooting in a school courtyard. Witnesses watched as the teen fled to a diner, where he stood outside and put the pistol to his head. The school went into a lockdown and sent students home. A nearby elementary school in the Southern Oregon town also was locked down as a precaution.

Source: [http://seattletimes.nwsources.com/html/localnews/2002824255\\_wenoreshooting23.html](http://seattletimes.nwsources.com/html/localnews/2002824255_wenoreshooting23.html)

[[Return to top](#)]

## **General Sector**

Nothing to report.

[[Return to top](#)]

## **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS Daily Report Team at (703) 983–3644.
Subscription and Distribution Information:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.